PANELLIST’S STATEMENT:
DAVID F C BREWER, Gamma Secure Systems Limited

Dr. David Brewer
Gamma Secure Systems Limited[1]
Diamond House
149, Frimley Road
Camberley, Surrey
GU15 2PS
United Kingdom

Tel: +44-1276-691415 Fax: +44-1276-692903
E-mail: dbrewer@gammassl.co.uk

Quite apart from the Cabinet Office Review of Protective Security (RPS), there have been other changes which have propelled Information Security (IS) to the top of UK MoD’s agenda as a business risk management tool. This parallels recent changes in the commercial arena where the marketplace is demanding greater assurance of secure operation from payment and information services where high value is at stake (see Figure 1). The question that I would like to raise is whether this heralds a convergence between commercial and defence IS approaches or whether fundamental differences still remain.

Prior to RPS, the over-arching policy of ‘risk avoidance’ compelled the MoD and other government departments to seek multi-level security solutions that where undoubtedly beyond the state-of-the-art at the time. Understandably this led to some spectacular failures in the late 1980s and prompted a complete IS re-think. Moreover, the advent of the home computer in the early 1990s meant that MoD staff enjoyed computer power at home that was vastly superior to that which they could ever enjoy from a bespoke solution in the office. Clearly, the traditional acquisition methods for military hardware such as tanks and ships were rapidly becoming inappropriate for software intensive projects. In the UK, we concluded that for many applications, it might be possible to utilise commercial-of-the-shelf (COTS) technology. There were two imponderables: what level of security could we get? and could the products be reliably integrated together? Accordingly, in 1992 the MoD

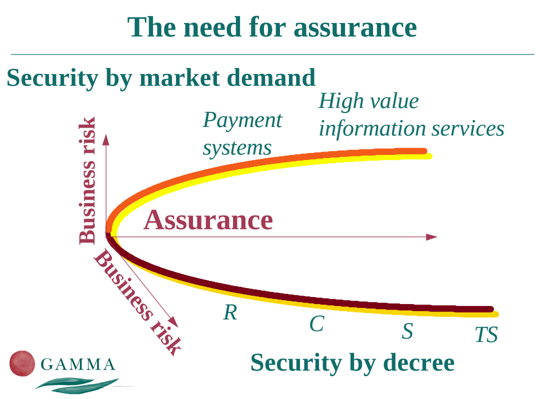


Figure 1

[1] Gamma is a leading UK information security consultancy which creates products and services to help customers gain assurance that their information security needs are met.

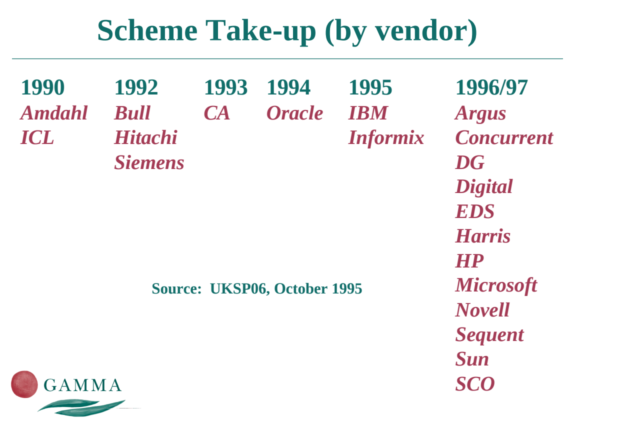
commissioned the Secure Open System Technical Demonstrator Programme (SOS TDP) to find out.

The adoption of RPS in April 1994 heralded a move from ‘risk avoidance’ to a ‘risk management’ approach to security. The threat had changed with the demise of the Soviet Bloc, but so had the theatre of operations. The concept of tension, transition to war, and then war itself, with no apparent transition back to peace, had been replaced by a cycle of rapid deployment, engagement, and re-deployment, followed by a comforting return to barracks. The need to rapidly acquire and assemble new information technology (IT), to meet the demands of some new deployment such as the Gulf War, were more important than ever before. Early SOS TDP results, coupled with the pragmatic approach to IS afforded by the RPS, indicated that this might be simply achieved with COTS products with ‘Orange Book’ class C2 functionality. However, other developments were to change that view entirely.

Firstly, a series of studies, that considered the IS requirements for a comprehensive range of MoD systems, concluded:

1. Most MoD systems operate in a system-high mode (i.e. user clearances exceed data classification), but labelling is required.
2. There are at least three different variations of the ‘system-high with labels’ policy, each one characteristic of a different type of MoD business.

Secondly, there was a major organisational change within the MoD which brought together the acquisition of peacetime and operational systems. This brought home the realisation that the peacetime and operational tasks were often closely related, and in some cases performed by the same people. The threats are different in the two environments but the information and ownership is the same. This highlighted the fact that the IS requirement was dependent on the business requirement. Indeed, this business requirement has been recently reviewed, taking a top down approach to determine how all current and future systems/functional areas should work together to form an effective whole.



Scheme Take-up (by vendor)

1990	1992	1993	1994	1995	1996/97
Amdahl	*Bull*	*CA*	*Oracle*	*IBM*	*Argus*
ICL	*Hitachi*			*Informix*	*Concurrent*
	Siemens				*DG*
					Digital
					EDS
					Harris
					HP
					Microsoft
					Novell
					Sequent
					Sun
					SCO

Source: UKSP06, October 1995

Figure 2: Date (or anticipated date) of ITSEC certification for various products

Finally, there have been major advances in technology and changes in MoD’s use of IT. In particular, interest in CALS and the Internet has highlighted the need for firewalls and cryptographic-based controls, such as electronic signatures and non-repudiation services. Moreover, 1995 saw a tremendous uptake in the UK ITSEC evaluation and certification scheme, as indicated in Figure 2. Soon, I would predict that trusted CMW-like platforms will become commonplace in the home environment to safely launch Visa/Mastercard and electronic cash payments, rather like a CMW can be used in a bank to enforce the traditional 'check and release' function. In some sense, therefore, secure commercial IT has overtaken the SOS TDP, which has a become a conduit for its introduction into MoD systems.

In view of these developments, MoD is in the process of rationalising its approach to IS in two ways: by adopting a common risk management approach across all functional areas, and by preparing properly for the Information Age. It is in this latter respect that IS as a business risk management tool will really come into its own. The MoD is currently developing a new approach to specifying IS requirements as a characteristic of 'business domains'. These domains transcend the traditional IT boundaries to take account of user awareness, and physical and procedural measures. As such, the approach lends itself to business risk management and should be extendible to embracing concepts such as British Standard BS7799, a forerunner of the Generally accepted System Security Principles (GSSP) initiative, as well as ITSEC, the Common Criteria and GSSP itself. Of perhaps greater interest is that these domains may interface with 'commercial domains', such as payment systems, and information systems such as CNN.